Agilent ICP-MS ChemStation – Complying with 21 CFR Part 11

Application Note

Overview

Part 11 in Title 21 of the Code of Federal Regulations includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The intent of these guidelines is to ensure that electronic records subject to these guidelines are reliable, authentic and maintained with high integrity.

This document examines each section of 21 CFR Part 11 and provides a recommended remediation approach using the Agilent ICP-MS ChemStation with User Access Control Pack enabled, in combination with the Agilent OpenLAB ECM solution for electronic records management.

The User Access Control Pack provides the necessary controls for managing system access and audit trail functionality while Agilent OpenLAB ECM ensures secure record keeping and data archival. Agilent OpenLAB ECM is proven and has been deployed at many leading life sciences companies to satisfy compliance mandates for 21 CFR Part 11.

	21 CFR 11 Sections (✔ = applicable / N/A = not applicable)									
Possible scenarios with ChemStation operated in a closed system	11.1 , 11.2 , 11.3	11.10	11.30	11.50	11.70	11.100	11.200 (a)	11.200 (b)	11.300 (a) , (b) , (d)	11.300 (c) , (e)
Electronic Record only (without signature)	✔	✔	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Electronic Signature Based upon ID Code & Password	✔	✔	N/A	✔	✔	✔	✔	N/A	✔	N/A

Figure 1
Applicable sections of 21 CFR Part 11

Agilent Technologies

11.10 Controls for Closed Systems

Section	Result	Question	Answer
11.10a	Yes	*Has the system been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?*	Agilent develops its products according to the well established “product lifecycle” concept, which is a phase review process for soft- and hardware development, in order to ensure consistent product quality. As a result a fully qualified data handling system is delivered together with all necessary services, which are needed to implement such a system to meet the requirements of the FDA regarding 21CFR Part11. As part of this service a document is compiled that describes the installed configuration and documents the results of the executed IQ and OQ procedures. Electronic records generated by the ICP-MS ChemStation are securely stored in OpenLAB ECM. OpenLAB ECM's performance has been extensively validated with tests written to specifically evaluate accuracy, reliability and consistent performance. OpenLAB ECM incorporates the use of byte order dependant check sums at each file transfer operation to ensure that records are valid and unaltered.
11.10b	Yes	*Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by the FDA?*	Electronic records are created in electronic as well as human-readable form. OpenLAB ECM stores all data types, from raw machine data to printable reports. All files are stored complete and unaltered in the original format. To read the electronic format the Agilent ICP-MS ChemStation is required. “Printed” reports, representing the human-readable form of electronic records, can be stored as PDF files which can be made available for review without the source application being installed on the client machine. An MS viewer is available to view the original electronic record without the originating application.
11.10c	Yes	*Are the records protected to enable the accurate and ready retrieval throughout the record retention period?*	Raw, meta and result data generated by the Agilent ICP-MS ChemStation are stored and managed in OpenLAB ECM. It resides in a protected storage location and/or archive media. When archived, the media may be on-line, near-line or off-line. Regardless of the physical location of the data, it remains searchable to all users with appropriate privilege. The individual users do not need access to the physical storage location of the files.
11.10d	Yes	*Is system access limited to authorized individuals?*	Each user is identified by a unique user-ID/password combination. Logging on to the ICP-MS ChemStation requires the entry of both identification components. The Windows user management is used for setting up authorized users and assigning user privileges. Users gain access to the ICP-MS ChemStation by being added to one of the three ChemStation user groups that are created upon installation. Access

Section	Result	Question	Answer
			to data maintained in OpenLAB ECM is controlled through a user name, password, and account login. The user management can be integrated with the Windows user management. Once inside the OpenLAB ECM repository, all file and software functionality access is controlled through privileges and roles assigned to individual users or groups of users. Setting up and maintaining users as well as specifying security policies and determining the level of access is the responsibility of the system administrator using standard Windows administration functionality (e.g. forcing users to specify a new password during the first logon, defining password expiration periods, number of logon attempts until account is locked etc.) The Windows lock function locks the session after a specified period of inactivity. The timeframe is configurable by the system administrator. Both identification components are required to start a new session when the inactivity timeout locks the session in order to regain access to the system.
11.10e	Yes	*Is there a secure, computer-generated, time-stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records?*	Logon and logoff to the ICP-MS ChemStation is documented in the Windows application log. All OpenLAB ECM activities (e.g. data storage, versioning, electronic signatures) are recorded in a secure, computer generated, time stamped audit trail. Entries in the OpenLAB ECM audit trail are non-editable, non-deletable. The user has no influence on the audit trail, e.g. it cannot be switched off or altered nor deleted. Removing records from the database does not affect existing entries in the audit trail. The audit trail lists all modifications with date/time stamp and the user name of the user doing the change.
11.10e	Yes	*When records are changed, is previously recorded information left unchanged?*	All entries in the OpenLAB ECM audit trail are non-editable, non-deletable. Removing records from the database does not affect existing entries in the audit trail.
11.10e	Yes	*Are electronic audit trails kept for a period at least as long as their subject electronic records and available for agency review and copying?*	Audit trail entries are stored in the OpenLAB ECM repository as part of a file's metadata and are kept throughout the electronic records retention period. The audit trail may be reviewed and printed. The Windows application log can also be stored in the same OpenLAB ECM repository.
11.10(f)	Yes	*Are operational system checks used to enforce permitted sequencing of steps and events?*	In all ICP-MS ChemStation and OpenLAB ECM functions, when a sequencing of events is required, system checks enforce it.

Section	Result	Question	Answer
11.10(g)	Yes	*Are authority checks in place to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand?*	Each user must logon to the software with a user ID / password combination before they can use the system. This applies at initial program start and after every inactivity timeout on the computer program. Only a successful logon to the system offers access to the chromatographic software functions such as data acquisition, data review, result approval or archiving functionality. Users cannot gain access to OpenLAB ECM without a valid user name, password and account. Once logged in, that user's access to files and software functionality (including but not limited to signing a file, inputting values, or altering a record) are determined by the privileges assigned.
11.10(h)	Yes	A*re device checks used to determine, as appropriate, the validity of the source of data or operational instruction?*	User entry fields provide feedback to the user about the entry types and ranges that are valid for that field.
11.10(i)	Yes	*Do the persons who develop, maintain, or use electronic records/signature systems have the education, training, and experience to perform their assigned tasks?*	Records of the educational and employment history of employees are verified and kept with personnel records that can be made available during an on-site audit. In addition, all Agilent Technologies employees who deal with regulations have attended training workshops on regulatory requirements. For system users Agilent provides a basic familiarization during the installation of the product. Training courses for administrators as well as users are available.
11.10(j)	N/A	*Have written policies been established, and adhered to, that hold individuals accountable and responsible for actions initiated under their e-signatures in order to deter record and signature falsification?*	It is the responsibility of the organization implementing electronic signatures to develop written policies that ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature.
11.10(k) (1)	N/A	*Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?*	While documentation is available for ICP-MS ChemStation and OpenLAB ECM users and administrators; controls over the storage and distribution of this material are the responsibility of the organization that implements and uses the system.
11.10(k) (2)	N/A	*Are there formal revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation?*	The quality process includes formal written revision and change control procedures for system documentation. OpenLAB ECM can be used for development and maintenance of system documentation. All revisions to the documents are kept time stamped and audit trailed.

11.30 Controls for Open Systems

A closed system is required. Agilent ICP-MS ChemStation is not designed to operate as an open system.

Section	Result	Question	Answer
11.30	N/A	*Are there procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt?*	When a file is transferred to or within OpenLAB ECM, a byte order dependant checksum is calculated on the file in its source location. A copy of the file is made of the file in the destination location where a second checksum is calculated. The two values are compared and only if they are identical, is the transfer complete. If the values do not match, an error message is generated.
11.30	N/A	*Are additional measures used to ensure the confidentiality of the electronic records from the point of their creation to the point of their receipt?*	OpenLAB ECM supports the use of Secure Socket Layer (SSL) encryption for security during data transmission. SSL breaks a single file into very small data packets. These data packets are individually encrypted with configurable 64-bit or 128–bit encryption before being transmitted. On the receiving side the data packets are decrypted and reassembled.

11.50 Signature Manifestation

Section	Result	Question	Answer
11.50 (a)	Yes	*Do the signed electronic records contain information associated with the signing that clearly indicates the following:* *1. Printed name of signer,* *2. Date and time that the signature was executed* *3. The meaning associated with the signature?*	OpenLAB ECM 's electronic signature manifestation includes: 1. User name in addition to the full name of the signer 2. Signer's title 3. Date and time that the signature was applied 4. Location where the signing occurred 5. User configurable meaning associated with the signature
11.50 (b)	Yes	*Are these items part of any human readable form of the electronic record?*	The eSignature Plug-in for Adobe Acrobat places a visible signature manifestation on all human readable forms of the document, electronic display and printed form.

11.70 Signature / Record Linking

Section	Result	Question	Answer
11.70	Yes	*Is the electronic signature linked to its respective electronic record to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means?*	The eSignature Plug-in for Adobe Acrobat encrypts the signature within the document to prevent the signature from being excised or copied to another document. OpenLAB ECM will not recognize a signature that was applied outside its own electronic signature plug-ins.

11.100 Electronic Signatures: General Requirements

Section	Result	Question	Answer
11.100 (a)	Yes	*Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?*	OpenLAB ECM uses the user name / password combination (unique to each user) in the electronic signature feature. User names within OpenLAB ECM are required to be unique and cannot be reused or reassigned to another individual.
11.100 (b)	N/A	*Are the identities of the individuals verified prior to the establishment, assignment, and certification or otherwise sanctioning an individual's electronic signature or any element of an electronic signature?*	This is the responsibility of the organization, which plans, implements and operates the system. Such a verification process is a system requirement that is set before implementing electronic signature procedures and / or assigning electronic signature privileges to an individual.
11.100 (c)	N/A	*Has the company delivered its corporate electronic signature certification letter to FDA?*	It is the company's responsibility, before submitting electronically signed documentation to the FDA, to register their intent to use electronic signatures. In addition, training programs must be in place to ensure that users signing documents electronically understand the legal significance of their electronic signature.
11.100 (c)(1)	N/A	*Is it in paper form with a traditional handwritten signature?*	This is the responsibility of the organization, which operates the system. See 11.100(c).
11.100 (c)(2)	N/A	*Can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?*	This is the responsibility of the organization, which operates the system. See 11.100(c).

11.200 Electronic Signature Components and Controls.

Section	Result	Question	Answer
11.200 (a)(1)	Yes	*Does the e-signature employ at least two distinct identification components such as user ID and password?*	The OpenLAB ECM electronic signature tools consist of two components, user ID (unique) and password.
11.200 (a)(1)(i)	Yes	*When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components?*	When an individual signs the first of a series of documents during a single period of controlled access the user is required to enter both signature components; user ID/ password.
11.200 (a)(1)(i)	Yes	*When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed*	When a OpenLAB ECM user executes a series of continuous electronic signatures (defined as signatures executed within a system administrator determined period of time) they are required to enter user ID, password and reason on the first signature only. Each subsequent signature requires

Section	Result	Question	Answer
		using at least one electronic signature component that is only executable by, and designed to be used by, the individual?	only the user's password, which is known only to the user.
11.200 (a)(1)(ii)	Yes	*When an individual executes a series of signings not performed during a single, continuous period of controlled system access; does each signing executed require all signature components?*	When a Cerity ECM user executes a series of non-continuous electronic signatures (defined as signatures executed outside of a system administrator determined period of time) they are required to enter user ID, password and reason on each signature.
11.200 (a)(2)	Yes	*Are controls in place to ensure that only their genuine owners can use the electronic signature?*	Cerity ECM can be configured such that an administrator can assign an initial password to a user for new account or forgotten password, but the user is required to change that password on their first login. In this manner the user ID/password combination is known only to the individual.
11.200 (a)(3)	Yes	*Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals?*	Cerity ECM uses the user's user ID and password to initiate the electronic signature. An Cerity ECM user's password is stored encrypted within the database and is displayed as asterisks in all location within the software. The system administrator should only know user IDs as he sets up the users. During setup he can force a password change during the first logon. Then the password is only known to the individual users as it is defined at each user's individual first logon. See also 11.200(a)(2). The enforcement is the responsibility of the organization, which operates the system. Thus it requires active collaboration with the purpose of sharing passwords to enable irregular use of somebody else' identification.
11.200 (b)	N/A	*Are electronic signatures based on biometrics designed to ensure that only their genuine owners can used them?*	Cerity ECM does not support signatures based on biometrics at this time.

11.300 Controls for Identification Codes / Passwords

Section	Result	Question	Answer
11.300 (a)	Yes	*Are controls in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password?*	The company's Windows™ logins are used to validate users, so no two users can have the same user ID/password combination.

Section	Result	Question	Answer
11.300 (b)	Yes	*Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised?*	Password renewal interval is configured as part of the Windows password policy setup. The administrator can define that passwords are automatically, periodically revised and users are prevented from reusing passwords.
11.300 (c)	N/A	*Are there loss management procedures in place to electronically disable lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information?*	Neither the ICP-MS ChemStation nor Cerity ECM support devices that bear or generate identification codes (such as tokens or cards) at this time.
11.300 (d)	Yes	*Are transaction safeguards in use to prevent unauthorized use of passwords and/or identification codes?*	The system can be configured such that only the user knows their user ID/password identification code. Passwords are always displayed as asterisks and are stored encrypted within the database so that even an administrator cannot see them.
11.300 (d)	Yes	*Are transaction safeguards in use to detect and report in an immediate and urgent manner, any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management?*	The Windows security policy can be configured such that a user defined number of unauthorized access attempts lock out the user account and send email notification to a system administrator. The system audit trail documents general events such as logon attempts to the computer as well as the application or user changes, in the Windows Event logs as a central audit repository for all security information. This includes the system and computer ID along with the operator name and application identification, allowing for an immediate check of the potential security leak.
11.300 (e)	N/A	*Are there controls in place to initially test devices that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?*	Neither the ICP-MS ChemStation nor Cerity ECM support devices that bear or generate identification codes (such as tokens or cards) at this time.

www.agilent.com/chem/cds

References

Improving 21 CFR Part 11 Compliance with Cerity ECM, *Agilent Application Note, publication number 5989-1750EN*, **2005.**

Published November 1, 2007
Publication Number 5989-4850EN

Agilent Technologies